

# PRODUCT OF LOCAL POINTS OF SUBVARIETIES OF ALMOST ISOTRIVIAL SEMI-ABELIAN VARIETIES OVER A GLOBAL FUNCTION FIELD

CHIA-LIANG SUN

- Physical Address: Institute of Mathematics, Academia Sinica, 6F, Astronomy-Mathematics Building, No. 1, Sec. 4, Roosevelt Road, Taipei 10617, TAIWAN
- E-mail Address: `csun@math.sinica.edu.tw`

ABSTRACT. For a semi-abelian variety over a global function field which is isogenous to an isotrivial one, we show that on the product of local points of a subvariety satisfying a minor condition, the topological closure of a finitely generated subgroup of global points cuts out exactly the global points of the subvariety lying in this subgroup. As a corollary, on every non-isotrivial super-singular curve of genus two over a global function field, we conclude that the Brauer-Manin condition cuts out exactly the set of its rational points.

## 1. INTRODUCTION

Let  $K$  be a global function field of characteristic  $p$ , that is, a finitely generated field extension over the prime field  $\mathbb{F}_p$  with the transcendence degree 1. We fix an algebraic closure  $\overline{K}$  and let  $K^s$  denote the separable closure of  $K$ . Let  $\Omega_K$  denote the set of all places of  $K$  and let  $\Omega$  denote a co-finite subset of  $\Omega_K$ . For each  $v \in \Omega_K$ , let  $K_v$  denote the completion of  $K$  at  $v$ . For an algebraic variety  $X$  defined over  $K$ , we endow  $X(K_v)$  with the natural  $v$ -adic topology, and then endow  $\prod_{v \in \Omega} X(K_v)$  with the product topology. In this paper, we assume that  $X$  is a closed subvariety of a given semi-abelian variety  $A$ , both are defined over  $K$ . We identify every subset  $H \subset A(K)$  as a topological subspace of  $\prod_{v \in \Omega} A(K_v)$  by the diagonal embedding, and denote by  $\overline{H}$  its topological closure; moreover, for each  $v \in \Omega_K$ , the inclusion  $H \rightarrow A(K_v)$  is continuous and therefore induces a subtopology of  $H$ , which will be referred to as  *$v$ -adic subtopology*.

Suppose  $H$  is a subgroup of  $A(K)$ . The main aim of this paper is to investigate the circumstances where the equality

$$(1) \quad \prod_{v \in \Omega} X(K_v) \cap \overline{H} = X(K) \cap H$$

holds. To do so, we shall assume that  $H$  is *finitely generated*, as Example 0 in Subsection 3.3 shows that the equality would not hold even in the simplest case where  $A = \mathbb{G}_m$ , otherwise. On the other hand, the case where  $A$  is an abelian variety and  $H = A(K)$ , has been studied by Poonen and Voloch [PV10]. Indeed, they propose that in general the equality

$$\prod_{v \in \Omega} X(K_v) \cap \overline{A(K)} = \overline{X(K)}$$

should hold, and they prove (1) under the hypothesis that  $A_{\overline{K}}$  has no isotrivial quotient,  $A(K^s)[p^\infty]$  is finite and  $X$  is coset-free (*op. cit.*, Conjecture C and Theorem B). In this paper, we consider the case where  $A$  is isogenous to an isotrivial semi-abelian variety. Recall that in the category of varieties (resp. of semi-abelian varieties), an object defined over  $K$  is *isotrivial* if it is isomorphic over  $\overline{K}$  to one defined over  $\overline{\mathbb{F}_p}$ . Our main result is the following:

**Theorem 1.** *Let  $X$  be a closed subvariety of a semi-abelian variety  $A$ , both are defined over  $K$ . Assume that there is an isogeny  $f$  defined over  $\overline{K}$  from  $A$  to a semi-abelian variety  $A_0$  defined over  $\overline{\mathbb{F}_p}$  so that each translate  $P + f(X)$ ,  $P \in A_0(\overline{K})$ , of  $f(X)$  contains no positive-dimensional closed subvariety which is  $\overline{\mathbb{F}_p}$ -rational in  $(A_0)_{\overline{\mathbb{F}_p}}$ . Then for every finitely generated subgroup  $H$  of  $A(K)$ , the set  $X(K) \cap H$  is finite and the equality (1) holds.*

Example 1 at the end of Section 4 explains why we cannot expect the conclusion of our main result to hold without any assumption on  $X$ . The proof of the theorem consists of two parts which are carried out respectively in Section 3 and Section 4, with the key ingredients, Proposition 2, Lemma 9 and Lemma 10, proved in Section 5. The first part treats the case where  $X$  is zero-dimensional by adapting the proof of Proposition 3.7 in [PV10] to our situation, while the second reduces the general case to the zero-dimensional case by the induction on the dimension of  $X$  using a different Mordell-Lang type argument. The approach for the second part is originated from the proof of Theorem A. Part 1 in [AV92].

Suppose  $A$  is the Jacobian of  $X$  which is embedded into  $A$  under an Albanese map induced from a divisor on  $A$  defined over  $K$  of degree 1. It is proved in [PV10], Section 4, that if the Tate-Shafarevich group  $\text{III}(A)$  of  $A$  is finite, then the set  $\prod_{v \in \Omega_K} X(K_v) \cap \overline{A(K)}$  is in bijection with the Brauer set of  $X$  over  $K$ . Therefore, if Theorem 1 holds, then the Brauer-Manin condition cuts exactly the set of its  $K$ -rational points on  $X$ . An non-isotrivial projective curve can have its Jacobian isogenous to an isotrivial abelian variety; for examples, super-singular curves of genus 2 have this property [MB81]. The following corollary is proved in Section 4.

**Corollary 1.** *On any non-isotrivial projective  $K$ -curve with its Jacobian isogenous to an isotrivial abelian variety, the Brauer-Manin condition cuts exactly the set of its  $K$ -rational points.*

## 2. PRELIMINARIES

2.1. A semi-abelian variety  $A$  is said to be defined over a subfield  $F$  of  $\overline{K}$  if the underlying variety has the following form

$$(2) \quad \left\{ P \in \mathbb{P}^N(\overline{K}) : \begin{array}{l} f(P) = 0 \text{ for all } f \in I \\ g(P) \neq 0 \text{ for some } g \in J \end{array} \right\},$$

where  $I$  and  $J$  are homogeneous ideals in the polynomial ring  $F[X_0, \dots, X_N]$ , such that the group laws are expressible in  $F$ . For any field  $L$  such that  $F \subset L \subset \overline{K}$ , we say a closed subvariety of  $A$  is  *$L$ -rational in  $A_F$*  if, whenever  $A$  is expressed as (2), it has the form

$$\left\{ P \in \mathbb{P}^N(\overline{K}) : \begin{array}{l} f(P) = 0 \text{ for all } f \in \tilde{I} \\ g(P) \neq 0 \text{ for some } g \in J \end{array} \right\}$$

for some homogeneous ideal  $\tilde{I}$  in  $L[X_0, \dots, X_N]$ .

For each  $v \in \Omega_K$ , we denote by  $O_v$  the valuation ring in  $K_v$  and by  $m_v$  the maximal ideal in  $O_v$ . For a finite subset  $S$  of  $\Omega_K$ , the subring of  $S$ -integers in  $K$  is denoted by

$$O_S = \{x \in K : x \in O_v \text{ for each } v \notin S\}.$$

Given a such  $A$  defined over  $K$  as above, let  $J^{(v)}$  denote the subset of  $J \cap O_v[X_0, \dots, X_N]$  consisting of polynomials with some coefficients not in  $m_v$ , and define

$$(3) \quad A(O_v) = \left\{ P \in \mathbb{P}^N(K_v) : \begin{array}{l} P = [x_0 : \dots : x_N] \\ x_i \in O_v \text{ for all } i \\ x_{i_0} \notin m_v \text{ for some } i_0 \\ f(x_0, \dots, x_N) = 0 \text{ for all } f \in I \\ g(x_0, \dots, x_N) \notin m_v \text{ for some } g \in J^{(v)} \end{array} \right\}.$$

Also, for any finite subset  $S \subset \Omega$ , set

$$(4) \quad A(O_S) = \bigcap_{v \in \Omega_K \setminus S} (A(K) \cap A(O_v)).$$

Then, the following useful result can be obtained by Hilbert's Nullstellensatz:

**Lemma 1.** *Let  $\phi : A \rightarrow A$  be a regular map defined over  $K$ . Then  $\phi$  preserves  $A(O_v)$  for all but finitely many  $v \in \Omega_K$ , and hence  $A(O_S)$  for  $S$  sufficiently large.*  $\square$

2.2. The group operations on  $A$ , given by regular maps defined over  $K$ , are continuous with respect to the topology on  $A(K_v)$ , for each  $v \in \Omega_K$ . This implies that  $A(K_v)$  is a Hausdorff topological abelian group. It is totally disconnected since  $v$  is non-archimedean. Also, (3) shows that  $A(K_v)$  contains  $A(O_v)$  as a compact open subset. Consequently, it is locally compact, and hence complete. By Theorem (7.7), [HR79], it follows that the topology of  $A(K_v)$  is generated by open subgroups, and therefore so are  $\prod_{v \in \Omega} A(K_v)$  and its subgroups.

**Lemma 2.** *Every finitely generated subgroup  $H$  of  $A(K)$  admits a Hausdorff subtopology generated by subgroups with finite index.*

*Proof.* Because  $H$  is finitely generated and  $\Omega_K \setminus \Omega$  is finite, there exists a place  $v_0 \in \Omega$  such that  $A(O_{v_0})$  is a group containing  $H$ . Since  $A(O_{v_0})$  is a compact subgroup of  $A(K_{v_0})$  whose topology is Hausdorff and generated by subgroups, the topology of  $A(O_{v_0})$  is Hausdorff and generated by subgroups with finite index, and so is the  $v_0$ -adic subtopology of  $H$ .  $\square$

Let  $\mathfrak{P}(A, X, f, K)$  stand for the statement of Theorem 1.

**Lemma 3.** *Let  $A, X, f, K$  be as in Theorem 1 and let  $L/K$  be a finite extension. Then  $\mathfrak{P}(A, X, f, L) \Rightarrow \mathfrak{P}(A, X, f, K)$ .*

*Proof.* Note that the definition of  $\overline{H}$  depends on the choice of  $K$ . Let  $\Omega_L^0$  denote the set of places of  $L$  lying above  $\Omega$ . Consider the natural embeddings

$$H \hookrightarrow \prod_{v \in \Omega} A(K_v) \xrightarrow{i} \prod_{u \in \Omega_L^0} A(L_u).$$

Since  $i$  actually identifies  $\prod_{v \in \Omega} A(K_v)$  as a closed subgroup of  $\prod_{u \in \Omega_L^0} A(L_u)$ ,  $\overline{H}$  will be remained the same, if  $K$  is replaced by  $L$ . If  $\mathfrak{P}(A, X, f, L)$  holds, then

$\prod_{w \in \Omega_L^0} X(L_w) \cap \overline{H} = X(L) \cap H$  is a finite set. This implies

$$\begin{aligned}
& \prod_{v \in \Omega} X(K_v) \cap \overline{H} \\
&= \left( \prod_{w \in \Omega_L^0} X(L_w) \cap \prod_{v \in \Omega} A(K_v) \right) \cap \overline{H} \\
&= \prod_{w \in \Omega_L^0} X(L_w) \cap \overline{H} \\
&= X(L) \cap H \\
&= (X(L) \cap A(K)) \cap H \\
&= X(K) \cap H,
\end{aligned}$$

which is also a finite set.  $\square$

2.3. In view of Lemma 3, by replacing  $K$  by certain finite extension  $L$  if necessary, we can assume that  $A$  is an extension of an abelian variety  $B$  by a split torus  $\mathbb{G}_m^n$ , for some  $n \geq 0$ . This is actually the definition taken by Serre [Ser88]. Lemma 1 implies that  $A(O_v)$  is a group for all but finitely many  $v \in \Omega_K$ . Therefore, if  $S$  is sufficiently large, then  $A(O_S)$  is a subgroup of  $A(K)$ . In this case, it is finitely generated. To see this, we may extend  $S$  and assume that the subgroup  $\mathbb{G}_m^n(O_S) \subset A(O_S)$  coincides with  $(O_S^*)^n$ . Since  $A(O_S)$  is mapped into  $B(K)$  with  $\mathbb{G}_m^n(O_S)$  as the kernel, the assertion follows from the Mordell-Weil theorem and Dirichlet's unit theorem. Also, if  $S$  is large enough, then the finitely generated subgroup  $H$  is contained in  $A(O_S)$ .

**Lemma 4.** *Every isotrivial semi-abelian variety  $A_0$  is isogenous (over  $\overline{K}$ ) to the product  $\mathbb{G}_m^{n_0} \times B_0$ , for some nonnegative integer  $n_0$ , where  $B_0$  is an abelian variety defined over  $\overline{\mathbb{F}_p}$ .*

*Proof.* We may assume that  $A_0$  is actually defined over  $\overline{\mathbb{F}_p}$ . Then there is a strictly exact sequence (see [Ser88])  $1 \rightarrow \mathbb{G}_m^{n_0} \rightarrow A_0 \rightarrow B_0 \rightarrow 0$ , in which  $B_0$  is an abelian variety defined over  $\overline{\mathbb{F}_p}$ . It remains to show that  $A_0$  is isogenous to  $\mathbb{G}_m^{n_0} \times B_0$ .

Recall that, for any pair  $(\mathbb{G}, T)$  of commutative algebraic groups, the set of isomorphism classes of commutative algebraic groups  $E$  along with the strictly exact sequence  $0 \rightarrow T \rightarrow E \rightarrow \mathbb{G} \rightarrow 0$  forms an abelian group  $\text{Ext}(\mathbb{G}, T)$  under the Baer sum. In fact,  $\text{Ext}$  is a bifunctor from the category of pairs of commutative algebraic groups to the category of abelian groups [Ser88]. It is routine to check that, for any commutative algebraic group  $E$  representing its class  $[E] \in \text{Ext}(\mathbb{G}, T)$ , and any positive integer  $m$ , there is a natural exact sequence

$$(5) \quad 0 \rightarrow T[m] \rightarrow E \rightarrow E^{(m)} \rightarrow 0$$

defined over an algebraic closure of a field of definition of  $E$ , where  $T[m]$  is the algebraic subgroup of  $m$ -torsion points in  $T$ , and  $E^{(m)}$  is a commutative algebraic group representing the class  $m[E] \in \text{Ext}(\mathbb{G}, T)$ . In our case, the isomorphism class  $[A_0]$  of  $A_0$  lies in  $\text{Ext}(B_0, \mathbb{G}_m^{n_0}) = \text{Ext}(B_0, \mathbb{G}_m)^{n_0}$ , where the equality holds because  $\text{Ext}$  is a bifunctor. One knows (e.g., the comments following Theorem 6 of Chapter VII in [Ser88]) that  $\text{Ext}(B_0, \mathbb{G}_m)$  is isomorphic to the dual abelian variety  $B_0'$  of  $B_0$ . In particular,  $[A_0]$  lies in  $(B_0'(\overline{\mathbb{F}_p}))^{n_0}$  which is a torsion group. Therefore  $m[A_0] = 0$ , for some  $m$ , and hence  $\mathbb{G}_m^{n_0} \times B_0 = A_0^{(m)}$  and the isogeny is provided by (5).  $\square$

### 3. THE ZERO-DIMENSIONAL CASE

In this section, we prove Theorem 1, by assuming  $\dim X = 0$ .

**3.1. A Uniform Filtration Over All  $v$ -adic subtopologies.** Suppose  $A_0$  is a semi-abelian variety defined over a finite field  $\mathbb{F}_q$  containing  $\mathbb{F}_p$ . Then the Frobenius morphism  $\text{Frob} : A_0 \rightarrow A_0$  is well defined, and if  $A_0$  is embedded as a subvariety of  $\mathbb{P}^N$  then  $\text{Frob}$  is simply the restriction of the Frobenius map on  $\mathbb{P}^N$ , sending  $[x_0 : \dots : x_N]$  to  $[x_0^q : \dots : x_N^q]$ . Thus,  $\text{Frob}$  preserves the group structure on  $A_0$  and it induces an injective map  $A_0(O_S) \rightarrow A_0(O_S)$ , which we also denote by  $\text{Frob}$  which is a group homomorphism, if  $A_0(O_S)$  is a group.

**Proposition 1.** *Suppose that  $f : A \rightarrow A_0$  is an isogenous defined over  $\overline{K}$  and  $A_0$  is an isotrivial semi-abelian variety. Then for any finitely generated subgroup  $H$  of  $A(K)$ , there exists a collection  $\{U_n : n \geq 1\}$  of subgroups of  $H$  with the following two properties:*

- (1) *For each  $v \in \Omega_K$  and each  $n \geq 1$ ,  $U_n$  is open in every  $v$ -adic subtopology of  $H$ .*
- (2)  *$\bigcap_{n \geq 1} U_n$  is contained in the torsion subgroup of  $H$ .*

*Proof.* Without loss of generality, we may replace  $K$  by one of its finite extensions and assume that  $f$  is defined over  $K$  and  $A_0$  is defined over  $\mathbb{F}_q \subset K$ . Since

$H \xrightarrow{f} f(H)$  is continuous with finite kernel, it is sufficient to show that  $f(H)$  precesses a family of open sets satisfying the properties correspondingly. Thus, we only need to consider the case where  $A = A_0$  and  $f$  is the identity map.

We claim that for each  $v \in \Omega_K$  and each  $n \geq 1$ , the subgroup  $U_n := \text{Frob}^n(A(K)) \cap H$  is open in the  $v$ -adic subtopology. Then, (2) holds, as

$$\bigcap_{n \geq 1} U_n \subset \bigcap_{n \geq 1} \text{Frob}^n(A(K)) \subset A\left(\bigcap_{n \geq 1} K^{p^n}\right)$$

and  $\bigcap_{n \geq 1} K^{p^n}$  is the maximal finite subfield of  $K$ .

To prove the claim, we first note that since there is no nontrivial purely inseparable finite extension of  $K$  inside  $K_v$ ,  $\text{Frob}^n(A(K_v)) \cap A(K) \subset \text{Frob}^n(A(K))$ , and hence  $\text{Frob}^n(A(K_v)) \cap H \leq U_n$ . Then it remains to show that  $\text{Frob}^n(A(K_v)) \cap H$  is open in the  $v$ -adic subtopology of  $H$ . It is clear that  $\text{Frob}^n(A(K_v))$  is closed in  $A(K_v)$ , and consequently the quotient space  $A(K_v)/\text{Frob}^n(A(K_v))$  is Hausdorff. Consider the map  $H \rightarrow A(K_v)/\text{Frob}^n(A(K_v))$  induced from the inclusion  $H \subset A(K_v)$ . It is continuous with respect to  $v$ -adic subtopology of  $H$ . Also, as it factors through  $A(O_S)/\text{Frob}^n(A(O_S))$ , for some finite  $S \subset \Omega_K$  such that  $H \leq A(O_S)$ , the image of the map is finite, whence discrete. This completes our proof.  $\square$

**3.2. Congruence Subgroup Property.** For an additive topological abelian group  $G$ , we say that  $G$  has the **congruence subgroup property** if the subgroup  $nG =: \{nP : P \in G\}$  is open for every positive integer  $n$ ; if  $G$  is finitely generated, then the following conditions are equivalent:

- (1)  $G$  has the congruence subgroup property.
- (2) Every subgroup of  $G$  of finite index is open.
- (3) Every subgroup of  $G$  is closed.

**Lemma 5.** *Let  $G$  be a finitely generated abelian topological groups. Let  $\Sigma$  be a set consisting of natural numbers, which is closed under multiplication, satisfying the condition that every subgroup of  $G$  of index in  $\Sigma$  is open. Then  $\Sigma$  also satisfying the corresponding condition for each subgroup  $H$  of  $G$ , namely, every subgroup of*

$H$  of index in  $\Sigma$  is open in  $H$ . In particular, if  $G$  has the congruence subgroup property, then so has  $H$ .

*Proof.* We may assume that each positive divisor of any element in  $\Sigma$  also lies in  $\Sigma$ . Let  $m \in \Sigma$  be the product of those natural numbers in  $\Sigma$ , each of which is the order of some elements in the finitely generated abelian group  $G/H$ . Then, for every  $n \in \Sigma$ , we have  $H \cap mnG \leq nH$ . Since  $mn \in \Sigma$ , it follows that  $mnG$  is open in  $G$ . This shows that  $nH$  is open in  $H$  and so is every subgroup of  $H$  with index  $n$ .  $\square$

**Lemma 6.** *Suppose that every finitely generated subgroup of  $A(K)$  has the congruence subgroup property. Then for any finitely generated subgroup  $H$  of  $A(K)$  and any subset  $J$  of  $A(K)$ , we have  $J \cap \overline{H} = J \cap H$ .*

*Proof.* Choose a finite subset  $S$  of  $\Omega_K$  such that  $H \leq A(O_S)$  and  $S \cup \Omega = \Omega_K$ . Since  $A(O_S)$  has the congruence subgroup property,  $H$  is closed in  $A(O_S)$ . Consequently,  $A(O_S) \cap \overline{H} = H$ . Now, since  $A(O_S) = A(K) \cap \bigcap_{v \in \Omega} A(O_v)$ , while  $A(O_v)$  is closed in  $A(K_v)$ ,  $A(O_S)$  is closed in  $A(K)$ , and hence  $A(K) \cap \overline{A(O_S)} = A(O_S)$ . This implies  $J \cap \overline{H} = J \cap A(K) \cap \overline{A(O_S)} \cap \overline{H} = J \cap A(O_S) \cap \overline{H} = J \cap H$ .  $\square$

For any subgroup  $J$  of  $G := \prod_{v \in \Omega} A(K_v)$ , its topological closure  $\overline{J}$  is also a subgroup. In fact, since the map  $q : G \times G \rightarrow G$  defined by  $(P, Q) \mapsto P - Q$  is continuous, the preimage  $q^{-1}(\overline{J})$  is a closed subset of  $G \times G$  containing  $J \times J$ , and thus contains  $\overline{J} \times \overline{J} = \overline{J} \times \overline{J}$ ; then  $q(\overline{J}, \overline{J}) = \overline{J}$  as desired. The following result generalizes Lemma 3.6 in [PV10].

**Lemma 7.** *If a finitely generated subgroup  $H$  of  $A(K)$  has the congruence subgroup property, then every torsion element of  $\overline{H}$  lies in  $H$ .*

*Proof.* Write  $H = T + F$ , where  $T$  is finite subgroup and  $F$  is torsion-free. Suppose  $a \in \overline{H} \setminus T$  with  $ma = 0$  for some nonzero integer  $m$ . Since  $T$  is finite, there exists an open subgroup  $U$  of  $\prod_{v \in \Omega} A(K_v)$  such that  $(T + U) \cap (a + U) = \emptyset$ . Since  $F$  is of finite index in  $H$ , by the congruence subgroup property of  $H$ , we may assume that  $U \cap H \subset F$ . Lemma 5 says that  $U \cap H$  also has the congruence subgroup property, thus there exists an open subgroup  $V$  of  $\prod_{v \in \Omega} A(K_v)$  such that  $V \cap U \cap H = m(U \cap H)$ . Because  $ma = 0$ , the continuity of the multiplication-by- $m$  map ensures the existence of an open subgroup  $W$  of  $U$  such that  $m(a + W) \subset U \cap V$ . Now since  $a \in \overline{H}$ , there exist  $t \in T$  and  $f \in F$  such that  $t + f \in H \cap (a + W)$ . Consequently,  $m(t + f) \in m(a + W) \cap H \subset U \cap V \cap H = m(U \cap H)$ , whence  $m(t + f) = mf'$  for some  $f' \in U \cap H \subset F$ . Then  $mt \in T \cap F = \{0\}$  and  $m(f - f') = 0$ , which implies  $f - f' \in T \cap F = \{0\}$  and  $f = f' \in U$ . This says  $t + f \in (T + U) \cap (a + W) \subset (T + U) \cap (a + U)$ , which is impossible.  $\square$

Suppose  $J \subset A(K)$  is a subgroup containing  $H$ . Then the inclusion  $J \rightarrow \overline{J}$  canonically induces a group homomorphism

$$(6) \quad J/H \rightarrow \overline{J}/\overline{H}.$$

**Lemma 8.** *Suppose every finitely generated subgroup of  $A(K)$  has the congruence subgroup property. Let  $H \leq J$  be subgroups of  $A(K)$ . If  $H$  is finitely generated, then (6) is injective. If furthermore the index  $[J : H]$  is finite, then (6) is actually an isomorphism.*

*Proof.* The first assertion follows from Lemma 6. The congruence subgroup property of  $J$  implies that if  $[J : H]$  is finite, then  $H$  is open in  $J$ . Thus,  $H = U \cap J$ , for some open subgroup  $U$  of  $\prod_{v \in \Omega} A(K_v)$ . Let  $y$  be an arbitrary point of  $\overline{J}$ . Then  $y \in z + U$  for some  $z \in J$ , and for any open subgroup  $V$  of  $U$ ,  $(y - z + V) \cap J \neq \emptyset$ . On the other hand, we have

$$(y - z + V) \cap J \subset (y - z + V) \cap (U \cap J) = (y - z + V) \cap H.$$

As the topology of  $\prod_{v \in \Omega} A(K_v)$  is generated by subgroups, it follows that  $y - z \in \overline{H}$ . This shows the surjectivity of (6).  $\square$

The proof of the following proposition is postponed to Subsection 5.1.

**Proposition 2.** *If  $A$  is isogenous to  $\mathbb{G}_m^N \times B$  for some nonnegative integer  $N$  and some abelian variety  $B$  defined over  $K$ , then every finitely generated subgroup of  $A(K)$  has the congruence subgroup property. In particular, the same conclusion holds if  $A$  is isogenous to an isotrivial semi-abelian variety defined over  $K$ .*

**3.3. The proof.** *Proof of Theorem 1 in the case where  $\dim X = 0$ :*

We write  $X = Z$  to reflect this zero-dimensional situation. As  $Z$  is zero-dimensional, by Lemma 3, we may replace  $K$  by a finite extension if necessary and assume that every point of  $Z$  actually belongs to  $Z(K)$ . In particular, the restriction  $i_v|_{Z(K)}$  of the natural map  $A(K) \xrightarrow{i_v} A(K_v)$  is a bijection.

In view of Lemma 6, we only have to show  $\prod_{v \in \Omega} Z(K_v) \cap \overline{H} \subset Z(K)$ . Let  $J$  be the subgroup of  $A(K)$  generated by  $H$  and  $Z(K)$ . By Proposition 1, there exists a collection  $\{U_n : n \geq 1\}$  of subgroups of  $J$ , which are open in every  $v$ -adic subtopology, such that  $\bigcap_{n \geq 1} U_n$  is contained in the torsion subgroup of  $J$ . Let  $Q = (Q_v)_{v \in \Omega}$ , with each  $Q_v \in Z(K_v)$ , denote an element of  $\prod_{v \in \Omega} Z(K_v)$ . Suppose  $Q$  is also contained in  $\overline{H}$ . Then there is a sequence  $\{P_n\}_{n \geq 1}$  in  $H$  such that at each  $v$ , the sequence  $\{i_v(P_n)\}_{n \geq 1}$  has  $Q_v$  as its limit point in  $A(K_v)$ . Write  $Q_{(v)} = i_v^{-1}(Q_v) \in Z(K)$ . Since each  $U_n$  is open in the  $v$ -adic subtopology, for each  $r \geq 1$ , there exists an  $N$  such that  $P_n - Q_{(v)} \in U_r$ , for  $n \geq N$ . It follows that for every pair  $v, w \in \Omega$ , the difference  $Q_{(v)} - Q_{(w)}$  belongs to  $\bigcap_{r \geq 1} U_r$ , whence a torsion point. Since the set  $\{Q_{(v)}\}_{v \in \Omega}$  is finite, there exists a non-zero integer  $m$  such that  $m(Q_{(v)} - Q_{(w)}) = 0$ , for each pair  $v$  and  $w$ . Fix a  $w \in \Omega$ . Then the difference  $Q - Q_{(w)} = (Q_v - Q_w)_{v \in \Omega} \in \overline{J}$  is torsion, and hence, by Proposition 2 and Lemma 7, it is actually contained in  $J$ . In particular,  $Q \in J$  is a global point.  $\square$

*Example 0.* The conclusion in Theorem 1 would fail, even in the case where  $\dim X = 0$ , if the hypothesis that  $H$  is finitely generated were removed. To see this, let  $K$  be the field  $\mathbb{F}_p(t)$  of rational functions over  $\mathbb{F}_p$ . Fix a place  $v_0$  of  $K$  such that  $t \notin \mathcal{O}_{v_0}$ . Let  $\alpha, \beta \in K^*$  with  $\beta - \alpha = \frac{a}{b}$ , where  $a, b \in \mathbb{F}_p[t]$ . Denote by  $Z$  the  $K$ -subvariety  $\{\alpha, \beta\}$  of  $\mathbb{G}_m$ , and by  $K^* \xrightarrow{i_v} K_v^*$  the natural inclusion. Consider the sequence

$$(7) \quad x_n = \frac{(\prod_{i=1}^n \pi_i)^n + a}{(\prod_{i=1}^n \pi_i)^{2n} + b} + \alpha,$$

where  $\pi_1, \pi_2, \pi_3, \dots$  are all irreducibles in  $\mathbb{F}_p[t]$ . Then the sequence  $(x_n)$  has a limit  $Q = (Q_v)_{v \in \Omega_K}$  in  $\prod_{v \in \Omega_K} K_v^*$ , where  $Q_{v_0} = i_{v_0}(\alpha)$  and  $Q_v = i_v(\beta)$  for every

$v \in \Omega_K \setminus \{v_0\}$ , because

$$x_n - \beta = \frac{(\prod_{i=1}^n \pi_i^n)(b - a \prod_{i=1}^n \pi_i^n)}{b(\prod_{i=1}^n \pi_i^{2n} + b)}.$$

- (i) If  $\alpha \neq \beta$ , then  $Q \in \prod_{v \in \Omega_K} Z(K_v) \cap \overline{\mathbb{G}_m(K)} \setminus Z(K)$ .
- (ii) Suppose  $\alpha = \beta \neq 1$  and set  $b = 1$  in (7). Then  $\{x_n : n \geq 1\} \not\subset O_S^*$  for any finite  $S \subset \Omega_K$ ; hence, by taking a subsequence, we may assume that every nonzero power of  $x_n$  does not belong to the subgroup of  $\mathbb{G}_m(K)$  generated by  $\{\alpha, x_1, \dots, x_{n-1}\}$ . Letting  $H$  be the subgroup of  $\mathbb{G}_m(K)$  generated by  $\{x_n : n \geq 1\}$ , we have  $Q \in \prod_{v \in \Omega_K} Z(K_v) \cap \overline{H} = Z(K) \cap \overline{H} \setminus H$ .

#### 4. THE INDUCTIVE STEP

In this section, we complete the proof of Theorem 1 by reducing the general case to the zero-dimensional case which is established in Subsection 3.3. Focusing on the case where the isogeny  $f$  is the identity map until the very end of the reduction, the following Lemma 9 and Lemma 10 are crucial to our inductive procedure. Their proofs, being long and independent of the rest materials in this section, will be postponed until Subsection 5.2.

**Lemma 9.** *Let  $N$  be a non-negative integer and  $m$  a natural number. For each  $v \in \Omega$ , let  $I_v$  be an ideal of  $K_v[X_0, \dots, X_N]$ , generated by elements of  $K_v^{p^m}[X_0, \dots, X_N]$ . Then  $\bigcap_{v \in \Omega} (I_v \cap K[X_0, \dots, X_N])$  is generated by elements of  $K^{p^m}[X_0, \dots, X_N]$ .*

**Lemma 10.** *Let  $N, m$  be non-negative integers. For each  $v \in \Omega_K$ , the ideal generated by those homogeneous polynomials in  $K_v[X_0, \dots, X_N]$  vanishing on a subset of  $\mathbb{P}^N(K_v^{p^m})$  is actually generated by elements in  $K_v^{p^m}[X_0, \dots, X_N]$ .*

Then applications of the above are in order.

**Proposition 3.** *Let  $m$  be a natural number. Let  $A_0$  be a semi-abelian variety defined over the largest finite subfield  $\mathbb{F}_q \subset K$ , and  $X$  a closed  $K$ -subvariety which is not  $K^{p^m}$ -rational in  $(A_0)_{\mathbb{F}_q}$ . Then there is a proper closed  $K$ -subvariety  $Y$  of  $X$  such that  $X(K_v) \cap A_0(K_v^{p^m}) \subset Y(K_v)$  for all  $v \in \Omega$ .*

*Proof.* Since  $X$  is not  $K^{p^m}$ -rational in  $(A_0)_{\mathbb{F}_q}$ , we have an embedding of  $A_0$  into some  $\mathbb{P}^N$  so that its underlying variety is

$$(8) \quad \left\{ P \in \mathbb{P}^N(\overline{K}) : \begin{array}{l} f(P) = 0 \text{ for all } f \in I \\ g(P) \neq 0 \text{ for some } g \in J \end{array} \right\}$$

for some homogeneous ideals  $I$  and  $J$  in  $\mathbb{F}_q[X_0, \dots, X_N]$ , and that  $X$  is defined by (8) with  $I$  replaced by a homogeneous radical ideal  $I_X$  in  $\overline{K}[X_0, \dots, X_N]$  generated by elements of  $K[X_0, \dots, X_N]$ , but not by those of  $K^{p^m}[X_0, \dots, X_N]$ . For each  $v \in \Omega$ , consider the ideal  $\tilde{I}_v$  in  $K_v[X_0, \dots, X_N]$  generated by homogeneous polynomials vanishing on the subset  $X(K_v) \cap A_0(K_v^{p^m})$  of  $\mathbb{P}^N(K_v)$ . Let  $Y$  be the closed subvariety of  $A_0$  given by (8) except  $I$  is replaced by the homogeneous ideal

$$I_Y := \left( \bigcap_{v \in \Omega} (\tilde{I}_v \cap K[X_0, \dots, X_N]) \right) \cap K^{p^m}[X_0, \dots, X_N].$$

Thus  $X(K_v) \cap A_0(K_v^{p^m}) \subset Y(K_v)$  for all  $v \in \Omega$ . We shall show  $Y \subsetneq X$  by showing

$$(9) \quad I_X \subsetneq \overline{K}[X_0, \dots, X_N] \cdot I_Y.$$



To do so, we first apply Lemma 10 to deduce that  $\tilde{I}_v$  is generated by elements in  $K_v^{p^m}[X_0, \dots, X_N]$ . Then by Lemma 9, we conclude that  $\bigcap_{v \in \Omega} (\tilde{I}_v \cap K[X_0, \dots, X_N])$  is generated by elements in  $K^{p^m}[X_0, \dots, X_N]$ , and that the right side of (9) equals to  $\overline{K}[X_0, \dots, X_N] \cdot \bigcap_{v \in \Omega} (\tilde{I}_v \cap K[X_0, \dots, X_N])$ . Since  $I_X$  is not generated by elements of  $K^{p^m}[X_0, \dots, X_N]$ , it proves (9).  $\square$

**Proposition 4.** *Let  $A_0$  be a semi-abelian variety defined over the largest finite subfield  $\mathbb{F}_q \subset K$ , and  $X$  be a positive-dimensional closed  $K$ -subvariety of  $A_0$  such that all the largest dimensional irreducible components of the translates  $X + P$ ,  $P \in A_0(\overline{K})$ , are not  $\overline{\mathbb{F}_p}$ -rational in  $(A_0)_{\mathbb{F}_q}$ . Let  $H$  be a finitely generated subgroup of  $A_0(K)$ , Then there exists a closed  $K$ -subvariety  $Y$  of  $X$  with a smaller dimension, satisfying  $\prod_{v \in \Omega} X(K_v) \cap \overline{H} \subset \prod_{v \in \Omega} Y(K_v)$ .*

*Proof.* Let  $\text{Frob} : A_0 \rightarrow A_0$  be the Frobenius endomorphism. By taking  $H_0 = A_0(O_S)$  for some large enough finite  $S \subset \Omega_K$ , we assert that there is a finitely generated subgroup  $H_0$  of  $A_0(K)$  such that  $H \leq H_0$  and  $\text{Frob}(H_0) \leq H_0$ . Since  $\prod_{v \in \Omega} X(K_v) \cap \overline{H} \subset \prod_{v \in \Omega} X(K_v) \cap \overline{H_0}$ , it is enough to prove the desired result under the additional hypothesis that  $\text{Frob}(H) \leq H$ .

Assume that  $X$  is irreducible. First we apply the argument in the proof of Theorem A. Part 1 in [AV92] using the Hilbert scheme associated to equivalent compactification of  $A_0$ , and conclude that there is a positive integer  $N$  such that for every  $\gamma \in H$  the translate  $X_\gamma = X - \gamma$  is not  $K^{p^N}$ -rational in  $(A_0)_{\mathbb{F}_q}$ . Therefore, Proposition 3 implies that there is a proper closed  $K$ -subvariety  $Y_\gamma$  of  $X_\gamma$  such that  $X_\gamma(K_v) \cap A(K_v^{p^N}) \subset Y_\gamma(K_v)$  for all  $v \in \Omega$ .

Since the Frobenius endomorphism gives rise to an injection  $H \xrightarrow{\text{Frob}^N} H$ , the index  $[H : \text{Frob}^N(H)]$  is finite, and hence Lemma 8 implies that there are finitely many  $\alpha_i$ 's in  $H$  such that  $\overline{H} = \bigcup_i (\alpha_i + \overline{\text{Frob}^N(H)})$ . Now,  $Y_{\alpha_i} + \alpha_i$  is a proper closed  $K$ -subvariety of  $X$  such that  $X(K_v) \cap (\alpha_i + A_0(K_v^{p^N})) \subset (Y_{\alpha_i} + \alpha_i)(K_v)$ , for all  $v \in \Omega$ . Then we prove the proposition by taking  $Y = \bigcup_i (Y_{\alpha_i} + \alpha_i)$ .

In general, write  $X = X_1 \cup \dots \cup X_m \cup \dots \cup X_{m+n}$  where each  $X_i$  is irreducible and  $\dim X_j = \dim X$ , for  $j = 1, \dots, m$ ;  $\dim X_i < \dim X$ , for  $i = m+1, \dots, m+n$ . Then, for  $j = 1, \dots, m$ , choose a closed proper  $K$ -subvariety  $Y_j$  of  $X_j$  satisfying  $X_j(K_v) \cap \overline{H} \subset Y_j(K_v)$  for all  $v \in \Omega$ . For  $i = m+1, \dots, m+n$ , simply put  $Y_i = X_i$ . Then we complete the proof by taking  $Y = \bigcup_i^{m+n} Y_i$ .  $\square$

*Proof of Theorem 1.* In view of Lemma 3, we may assume that the isogeny  $f : A \rightarrow A_0$  is defined over  $K$ , that  $A_0$  is defined over some finite subfield of  $K$ , and that every point in the kernel of  $f$  lies in  $A(K)$ . If  $\dim X = 0$ , then the theorem is proved in Subsection 3.3. In general, we prove by the induction on  $\dim X$ .

Write  $X_0 = f(X)$ . Proposition 4 applied to  $A_0$  ensures the existence of a closed  $K$ -subvariety  $Y_0$  of  $X_0$  of smaller dimension such that

$$\prod_{v \in \Omega} X_0(K_v) \cap \overline{f(H)} \subset \prod_{v \in \Omega} Y_0(K_v).$$

Write  $Y = f^{-1}(Y_0) \cap X$ . Then the above implies

$$\prod_{v \in \Omega} X(K_v) \cap \overline{H} \subset \prod_{v \in \Omega} X(K_v) \cap \prod_{v \in \Omega} f^{-1}(Y_0)(K_v) = \prod_{v \in \Omega} Y(K_v).$$

The assumption in Theorem 1 is preserved when  $X$  is replaced by  $Y$ , hence the induction hypothesis implies that  $Y(K) \cap H$  is finite and

$$\prod_{v \in \Omega} Y(K_v) \cap \overline{H} = Y(K) \cap H.$$

Therefore,

$$\prod_{v \in \Omega} X(K_v) \cap \overline{H} \subset Y(K) \cap H \subset X(K) \cap H \subset \prod_{v \in \Omega} X(K_v) \cap \overline{H}.$$

This completes the proof.  $\square$

In order to deduce Corollary 1 from Theorem 1, we need the following result.

**Lemma 11.** *Let  $C_1 \rightarrow C \rightarrow C_0$  be a chain of nonconstant maps between projective curves defined over  $\overline{K}$  with  $C$  smooth. Suppose that both  $C_0$  and  $C_1$  as well as the composition  $C_1 \rightarrow C_0$  are defined over  $\overline{\mathbb{F}_p}$ . Then  $C$  is also defined over  $\overline{\mathbb{F}_p}$ .*

*Proof.* The given chain of maps induces the following diagram of their function fields:

$$\begin{array}{ccc} \overline{\mathbb{F}_p}(C_1) & \longrightarrow & \overline{K}(C_1) \\ \downarrow & & \downarrow \\ & & \overline{K}(C) \\ \downarrow & & \downarrow \\ \overline{\mathbb{F}_p}(C_0) & \longrightarrow & \overline{K}(C_0), \end{array}$$

where both columns are finite extensions, and the maps in both rows are  $\otimes_{\overline{\mathbb{F}_p}} \overline{K}$ . To prove this lemma, since  $C$  is smooth, it suffices to find a field  $F$  with transcendence degree 1 over  $\overline{\mathbb{F}_p}$  such that  $F \otimes_{\overline{\mathbb{F}_p}} \overline{K}$  is  $\overline{K}$ -isomorphic to  $\overline{K}(C)$ . First we assume that  $\overline{\mathbb{F}_p}(C_1)$  is separable over  $\overline{\mathbb{F}_p}(C_0)$ . Let  $N$  be the normal closure of  $\overline{\mathbb{F}_p}(C_1)$  over  $\overline{\mathbb{F}_p}(C_0)$ . Identifying all fields involved as subfields of  $N \otimes_{\overline{\mathbb{F}_p}} \overline{K}$ , we take  $F = N \cap \overline{K}(C)$ . Galois theory shows that  $[N \otimes_{\overline{\mathbb{F}_p}} \overline{K} : \overline{K}(C)] = [N : F]$ . Since  $F \otimes_{\overline{\mathbb{F}_p}} \overline{K} \subset \overline{K}(C)$  and  $[N \otimes_{\overline{\mathbb{F}_p}} \overline{K} : F \otimes_{\overline{\mathbb{F}_p}} \overline{K}] \leq [N : F]$ , we conclude that  $F \otimes_{\overline{\mathbb{F}_p}} \overline{K} = \overline{K}(C)$  as desired.

In the general case, let  $L$  be the separable closure of  $\overline{\mathbb{F}_p}(C_0)$  in  $\overline{\mathbb{F}_p}(C_1)$ . The preceding argument yields a field  $F'$  with transcendence degree 1 over  $\overline{\mathbb{F}_p}$  such that  $F' \otimes_{\overline{\mathbb{F}_p}} \overline{K}$  is  $\overline{K}$ -isomorphic to  $\overline{K}(C) \cap (L \otimes_{\overline{\mathbb{F}_p}} \overline{K})$ . Since  $\overline{K}(C)$  is purely inseparable over  $\overline{K}(C) \cap (L \otimes_{\overline{\mathbb{F}_p}} \overline{K})$ , the property of the Frobenius map shows that  $\overline{K}(C) \cap (L \otimes_{\overline{\mathbb{F}_p}} \overline{K}) = \overline{K}(C)^q$  for some power  $q$  of  $p$ , and since  $\overline{\mathbb{F}_p}$  is perfect, the field  $F = F'^{\frac{1}{q}}$  is the one we look for.  $\square$

*Proof of Corollary 1.* Let  $X$  be a non-isotrivial smooth projective  $K$ -curve with its Jacobian  $J$  isogenous to an isotrivial abelian variety  $A_0$ . Without loss of generality, we can assume that  $A_0$  is defined over  $\overline{\mathbb{F}_p}$ . Denote by  $f : J \rightarrow A_0$  the isogeny

and by  $\check{f} : A_0 \rightarrow J$  its dual. Let  $m$  be the positive integer such that  $f \circ \check{f}$  is the multiplication-by- $m$  map on  $A_0$ , and  $\check{f} \circ f$  is the multiplication-by- $m$  map on  $J$ . In view of the discussion given in Section 1, we need to show that  $\text{III}(J)$  is finite and each translate  $f(X) + P$ ,  $P \in A_0(\overline{K})$  is not  $\overline{\mathbb{F}_p}$ -rational.

Now, since  $A_0$  is isotrivial,  $\text{III}(A_0)$  is finite, by Tate [Tat95]. Choose a prime  $l$  not dividing  $pm$ . The isogenies  $f$  and  $\check{f}$  induce a chain

$$\text{III}(J)[l^\infty] \rightarrow \text{III}(A_0)[l^\infty] \rightarrow \text{III}(J)[l^\infty]$$

of maps between the  $l$ -primary part of  $\text{III}(J)$  and of  $\text{III}(A_0)$  such that the composition is an isomorphism. In particular,  $\text{III}(A_0)[l^\infty] \rightarrow \text{III}(J)[l^\infty]$  is surjective, hence  $\text{III}(J)[l^\infty]$  is finite as  $\text{III}(A_0)[l^\infty]$  is. By another result of Tate [Tat95], it follows that  $\text{III}(J)$  is finite as desired.

Suppose  $C_0 := f(X) + P$  is  $\overline{\mathbb{F}_p}$ -rational in  $A_0$ . Write  $C = X + Q$ , for some  $Q \in f^{-1}(P)$  and let  $C_1$  be an irreducible component of the pre-image of  $C_0$  under  $A_0 \xrightarrow{m} A_0$ . Then Lemma 11 is applicable to the chain  $C_1 \xrightarrow{\check{f}} C \xrightarrow{f} C_0$ . Consequently,  $C$  is defined over  $\overline{\mathbb{F}_p}$ , and hence  $X$ , being isomorphic to  $C$ , is isotrivial. This is a contradiction.  $\square$

*Example 1.* The conclusion in Theorem 1 would fail if no hypothesis were put on  $X$ . To see this, let  $K$  be the field  $\mathbb{F}_p(t)$  of rational functions over  $\mathbb{F}_p$ , and  $H = \langle t \rangle$  be the cyclic subgroup of  $\mathbb{G}_m(K)$  generated by  $t$ . Take a cofinite subset  $\Omega$  of  $\Omega_K$  such that  $t \in O_v^*$  for every  $v \in \Omega$ . For any  $m \geq n$ , we have

$$t^{p^{m!}} - t^{p^{n!}} = \left( t^{p^{n!(\frac{m!}{n!} - 1)}} - t \right)^{p^{n!}}.$$

Thus, the sequence  $(t^{p^{n!}})_{n \geq 1}$  in  $H$  is Cauchy, and admits a limit  $Q = (Q_v)_{v \in \Omega}$  in  $\overline{H}$  by compactness. Note that  $Q_{v_{t-1}} = 1$ , where  $v_{t-1} \in \Omega$  is the unique one satisfying  $t - 1 \in m_{v_{t-1}}$ ; while  $Q_v \neq 1$  for each  $v \in \Omega \setminus \{v_{t-1}\}$ . Hence  $Q \in \prod_{v \in \Omega} \mathbb{G}_m(K_v) \cap \overline{H} \setminus \mathbb{G}_m(K)$ .

## 5. THE PROOFS OF KEY INTERMEDIATE RESULTS

**5.1. The proof of Proposition 2.** In this subsection, we fix a finitely generated subgroup  $H \subset A(K)$ . The number field counter part of the following lemma (for  $\Omega$  consisting of only non-Archimedean places) is just a reinterpretation of Theorem 1, [Che51], and it can actually be carried over to the function field case. I thank the referee for pointing out the present much shorter proof using Galois cohomology.

**Lemma 12.** *If  $A = \mathbb{G}_m$ , then every subgroup of  $H$  of index prime to  $p$  is open.*

*Proof.* In view of Lemma 5, we only need to consider the case where  $H = \mathbb{G}_m(O_T) = O_T^*$  for a finite  $T \subset \Omega_K$ . For any finite subset  $S \subset \Omega$ , consider the open subgroup  $U_S = \prod_{v \in S} 1 + m_v$  of  $\prod_{v \in S} K_v^*$ . We shall prove the lemma by showing that for any natural number  $m$  prime to  $p$ , there is some  $U_S$  such that  $O_T^* \cap U_S \subset (O_T^*)^m$ .

Now, Kummer theory gives rise to the following commutative diagram

$$\begin{array}{ccccc}
O_T^*/(O_T^*)^m & \hookrightarrow & K^*/(K^*)^m & \xrightarrow{\sim} & H^1(K, \mu_m) \\
\downarrow & & \downarrow & & \downarrow \\
\prod_{v \in \Omega} O_v^*/(O_v^*)^m & \hookrightarrow & \prod_{v \in \Omega} K_v^*/(K_v^*)^m & \xrightarrow{\sim} & \prod_{v \in \Omega} H^1(K_v, \mu_m),
\end{array}$$

where the two injections are clear. As the Galois group of  $K(\mu_m)/K$  is cyclic, by Lemma I.9.3 of [Mil06], the right vertical arrow is an injection, and hence so is the left one. Since  $O_T^*/(O_T^*)^m$  is finite, there exists a finite subset  $S \subset \Omega$  such that the left vertical arrow induces an injection  $O_T^*/(O_T^*)^m \hookrightarrow \prod_{v \in S} O_v^*/(O_v^*)^m$ . Hensel's lemma shows  $U_S \subset \prod_{v \in S} (O_v^*)^m$ , whence  $O_T^* \cap U_S \subset (O_T^*)^m$  as desired.  $\square$

**Lemma 13.** *If  $A = \mathbb{G}_m$ , then every subgroup of  $H$  of  $p$ -power index is open in the  $v$ -adic subtopology, for every  $v \in \Omega_K$ .*

*Proof.* Again, by Lemma 5, we only need to consider the case where  $H = O_T^*$ . Now, we have  $(O_T^*)^{p^e} = O_T^* \cap (K^*)^{p^e}$ , which is shown in the proof of Proposition 1 to be an open subgroup in  $O_T^*$  in the  $v$ -adic subtopology, for every  $v \in \Omega_K$ .  $\square$

**Corollary 2.** *If  $A = \mathbb{G}_m^N$ , then every finitely generated subgroup of  $A(K)$  has the congruence subgroup property.*  $\square$

In the case where  $A$  is an abelian variety, the first assertion of Proposition 2 is essentially proved by Milne, who generalizes a result of Serre [Ser71] in the case where  $K$  was a number field.

**Proposition 5.** *Suppose that  $A$  is an abelian variety defined over  $K$ . Then every subgroup  $H$  of  $A(K)$  has the congruence subgroup property.*

*Proof.* The case where  $H = A(K)$  is exactly Corollary 1, [Mil72]. Then other cases follow from Lemma 5.  $\square$

*Proof of Proposition 2:* Let  $H$  be a finitely generated subgroup of  $A(K)$ . We need to show that  $nH \subset H$  is open for every  $n$ . Suppose we are given the isogeny  $\phi : A \rightarrow \mathbb{G}_m^N \times B$ . It follows from Corollary 2 and Proposition 5 that  $\phi(H)$  has the congruence subgroup property. In particular  $mn\phi(H) \subset \phi(H)$  is an open subgroup, for every  $m$ . Denote

$$T = \ker \left[ A(K) \xrightarrow{\phi} \mathbb{G}_m^N(K) \times B(K) \right].$$

Since  $T$  is finite, Lemma 2 implies the existence of an open subgroup  $U$  of  $H$  of a finite index  $m$  such that  $U \cap T$  is trivial.

Now, since  $nmH + T = \phi^{-1}(nm\phi(H))$  is open in  $H + T = \phi^{-1}(\phi(H))$ , the subgroup  $H \cap (nmH + T)$  is open in  $H$ . Also, since  $nmH \subset mH \subset U$  and  $U \cap T$  is trivial, we see that  $U \cap (nmH + T) = nmH$ . Therefore  $nmH$  is open in  $H$ , and thus so is  $nH$ .  $\square$

**5.2. The proofs of Lemma 9 and Lemma 10.** Our tool for proving Lemma 9 and Lemma 10 is the iterative derivation. An iterative derivation on a field  $L$  is a sequence  $\{D^{(i)}\}_{i \geq 0}$  of elements in the  $L$ -algebra of additive endomorphisms on  $L$  such that

- (i)  $D^{(0)}$  is the identity operator.
- (ii)  $D^{(i)}(xy) = \sum_{j=0}^i D^{(j)}(x)D^{(i-j)}(y)$ , for  $i \geq 0$  and  $x, y \in L$ .
- (iii)  $D^{(i)}D^{(j)} = \binom{i+j}{i} D^{(i+j)}$  for  $i, j \geq 0$ , where  $D^{(i)}D^{(j)}$  denotes the composition of  $D^{(i)}$  and  $D^{(j)}$ , and the rational integer  $\binom{i+j}{i}$  is the binomial coefficient.

Assume that  $L$  is of characteristic  $p$ . Then the following Lucas's lemma (see, for example, [Sch39]), is useful for telling if  $\binom{i+j}{i} \neq 0$  in  $L$ . For each nonnegative integer  $i$ , let  $i = \sum_{n=0}^d i_n p^n$ ,  $0 \leq i_n < p$ , denote its base  $p$  expansion.

**Lemma 14.** *The binomial coefficient  $\binom{i}{j}$  is not divisible by  $p$  if and only if  $i_n \geq j_n$  for all  $n$ .  $\square$*

The defining property (iii) implies  $D^{(i)} \circ D^{(j)} = D^{(j)} \circ D^{(i)}$ . Also, repeated applications of the property (iii) gives

$$\prod_{n=0}^d \left( D^{(p^n)} \right)^{i_n} = c_i D^{(i)},$$

where

$$c_i = \prod_{n=0}^d \left[ \binom{\sum_{s=0}^n i_s p^s}{i_n p^n} \prod_{a=1}^{i_n} \binom{ap^n}{p^n} \right].$$

Now, Lemma 14 implies  $c_i \in L^*$ , and hence

$$(10) \quad D^{(i)} = c_i^{-1} \cdot \prod_{n=0}^d \left( D^{(p^n)} \right)^{i_n}.$$

Inspired by the proof of Claim 2.2.3, [Ogu78], we consider the operator

$$\Delta_m := \sum_{i=0}^{p^m-1} (-t)^i D^{(i)}$$

on  $L$  for some  $t \in L$  satisfying

$$(11) \quad D^{(i)}((-t)^j) = (-1)^i \binom{j}{i} t^{j-i} \quad \text{for each } i, j \geq 0.$$

For each  $m \geq 0$ , let  $L_m = \{x \in L : D^{(l)}(x) = 0, \text{ if } 1 \leq l < p^m\}$ , which is a subfield of  $L$ .

**Lemma 15.** *For every  $c \in L$  and every  $m \geq 0$ , the element  $\Delta_m(c) \in L_m$ .*

*Proof.* In view of (10), we only need to show that for every natural number  $s < m$ ,

$$D^{(p^s)}(\Delta_m(c)) = 0.$$

For simplicity, set  $j = p^s$ . It follows from the property (iii) and the assumption (11) that

$$D^{(j)}(\Delta_m(c)) = \sum_{i=0}^{p^m-1} \sum_{l=0}^j (-1)^l \binom{i}{l} \binom{i+j-l}{i} (-t)^{i-l} D^{(i+j-l)}(c).$$

Lemma 14 implies that  $\binom{i}{l} \binom{i+j-l}{i}$  is a multiple of  $p$  unless both  $i_n \geq l_n$  and  $j_n \geq l_n$  hold for all  $n$ , which occurs only when  $l \in \{0, j\}$ , since  $j_s = 1$  and  $j_n = 0$  for all  $n \neq s$ . We also note that in case where  $l = j$ , those terms with  $i < j$  vanish as  $\binom{i}{j} = 0$ . Putting these together, we obtain

$$\begin{aligned} & D^{(j)}(\Delta_m(c)) \\ &= \sum_{i=0}^{p^m-1} \binom{i+j}{i} (-t)^i D^{(i+j)}(c) + \sum_{i=0}^{p^m-1} (-1)^j \binom{i}{j} (-t)^{i-j} D^{(i)}(c) \\ &= \sum_{i=j}^{j+p^m-1} \binom{i}{j} (-t)^{i-j} D^{(i)}(c) + \sum_{i=j}^{p^m-1} (-1)^j \binom{i}{j} (-t)^{i-j} D^{(i)}(c) \\ &= \sum_{i=p^m}^{p^m+p^s-1} \binom{i}{p^s} (-t)^{i-p^s} D^{(i)}(c), \end{aligned}$$

where the last equality holds because  $1 + (-1)^j = 1 + (-1)^p = 0$  in  $K$ . Finally, since  $s < m$ , for every  $i$  satisfying  $p^m \leq i \leq p^m + p^s - 1$ , we have  $i_s = 0$ , and hence  $\binom{i}{p^s}$  is a multiple of  $p$ , by Lemma 14. Thus, each term in the last sum vanishes. This finishes the proof.  $\square$

For each  $i \geq 0$ , we extend  $D^{(i)}$  to an additive endomorphism on the polynomial ring  $L[X_0, \dots, X_N]$  by sending  $X_i$  to 0 for every  $i \in \{0, 1, \dots, N\}$ . It is easy to verify that for all  $i \geq 0$ ,  $f, g \in L[X_0, \dots, X_N]$ ,

$$D^{(i)}(fg) = \sum_{j=0}^i D^{(j)}(f) D^{(i-j)}(g),$$

and, for all  $m \geq 0$ ,

$$L_m[X_0, \dots, X_N] = \{g \in L[X_0, \dots, X_N] : D^{(l)}(g) = 0, \text{ if } 1 \leq l < p^m\}.$$

**Lemma 16.** *For any positive integer  $m$ , an ideal  $I$  of  $L[X_0, \dots, X_N]$  is generated by elements of  $L_m[X_0, \dots, X_N]$  if and only if the condition  $D^{(i)}(I) \subset I$  holds for all  $1 \leq i < p^m$ .*

*Proof.* Suppose  $D^{(i)}(I) \subset I$  for all  $1 \leq i < p^m$ . Let  $J$  be the ideal of  $L[X_0, \dots, X_N]$  generated by  $I \cap L_m[X_0, \dots, X_N]$ . To complete the proof, we only need to show  $I = J$ , as the implication in the opposite direction is clear. Choose a lexicographic order on the set of monomials in  $X_0, \dots, X_N$ . With respect to this order, for each non-zero polynomial  $f \in K[X_0, \dots, X_N]$ , the *degree* of  $f$  is defined to be the largest monomial appearing in the expression of  $f$  with a non-zero coefficient, and  $f$  is *monic* if this coefficient is 1.

Suppose that  $I \setminus J$  is a non-empty set and let  $f \in I \setminus J$  be an element of the smallest degree. We also choose  $f$  to be monic. Since  $D^{(i)}(1) = 0$ , for all positive integer  $i$ , the degree of  $D^{(i)}(f)$  is smaller than that of  $f$ . Consequently,  $D^{(i)}(f) \notin I \setminus J$ , by the choice of  $f$ . On the other hand, since for every  $1 \leq i < p^m$ ,  $D^{(i)}(f) \in D^{(i)}(I) \subset I$ , we must have  $D^{(i)}(f) \in J$ . Now, consider the element

$$g = f + \sum_{i=1}^{p^m-1} (-t)^i D^{(i)}(f) \in L[X_0, \dots, X_N].$$

By the above argument,  $g \in I$ , and by Lemma 15,  $g \in L_m[X_0, \dots, X_N]$ . Hence,  $g \in J$  and  $f = g - \sum_{i=1}^{p^m-1} (-t)^i D^{(i)}(f) \in J$ , a contradiction.  $\square$

Now we construct a desired iterative derivation on  $K$ . Choose an element  $t \in K$  such that  $K$  is a finite separable extension of the function field  $\mathbb{F}_p(t)$  of one variable over  $\mathbb{F}_p$ . Choose a place  $v_0 \in \Omega_K$  which restricts to a place  $w \in \Omega_{\mathbb{F}_p(t)}$

corresponding to a separable irreducible polynomial in  $\mathbb{F}_p[t]$  such that  $\mathbb{F}_p(t)_w = K_{v_0}$ . Let  $\alpha$  be a root of this polynomial. Then  $\mathbb{F}_p(t)_w$  is a natural subfield of  $\mathbb{F}_p(\alpha)((t - \alpha))$  and we have a tower  $\mathbb{F}_p(\alpha)(t) \subset K(\alpha) \subset \mathbb{F}_p(\alpha)((t - \alpha))$  of fields. By Remark 1 in [GV87], there exists an iterative derivation  $\{D_{K(\alpha)}^{(i)}\}_{i \geq 0}$  on  $K(\alpha)$  such that  $D_{K(\alpha)}^{(j)}((t - \alpha)^i) = \binom{i}{j}(t - \alpha)^{i-j}$  and  $(K(\alpha))^{p^m} = \{x \in K(\alpha) : D_{K(\alpha)}^{(l)}(x) = 0, \text{ if } 1 \leq l < p^m\}$ , for  $i, j, m \geq 0$ . Denoting by  $D_K^{(i)}$  the restriction of  $D_{K(\alpha)}$  on  $K$ , we get an iterative derivation  $\{D_K^{(i)}\}_{i \geq 0}$  on  $K$ . It is not hard to check that  $D_K^{(j)}(t^i) = \binom{i}{j}(t)^{i-j}$ , whence (11) holds for  $D = D_K$ . Also, from the separability assumption, we have  $K^{p^m} = \{x \in K : D_K^{(l)}(x) = 0 \text{ if } 1 \leq l < p^m\}$ , for  $m \geq 0$ . Moreover, using the fact  $[K : K^p] = p$ , one can show that for each  $i$ , the endomorphism  $D_K^{(i)}$  is continuous with respect to every place of  $K$ . Therefore, for each place  $v \in \Omega$ , we extend  $\{D_K^{(i)}\}_{i \geq 0}$  and obtain an iterative derivation  $\{D_{K_v}^{(i)}\}_{i \geq 0}$  on  $K_v$ .

*Proof of Lemma 9:* Since  $I_v$  is generated by elements of  $K_v^{p^m}[X_0, \dots, X_N]$ , which lie in the kernel of those  $D_{K_v}^{(i)}$  with  $1 \leq i < p^m$ , it follows that for these  $i$  we have  $D_{K_v}^{(i)}(I_v) \subset I_v$  for each  $v \in \Omega$ . But then

$$\begin{aligned} & D_K^{(i)}\left(\bigcap_{v \in \Omega} (I_v \cap K[X_0, \dots, X_N])\right) \\ & \subset \bigcap_{v \in \Omega} \left(D_{K_v}^{(i)}(I_v \cap K[X_0, \dots, X_N])\right) \\ & \subset \bigcap_{v \in \Omega} \left(D_{K_v}^{(i)}(I_v) \cap K[X_0, \dots, X_N]\right) \\ & \subset \bigcap_{v \in \Omega} (I_v \cap K[X_0, \dots, X_N]) \end{aligned}$$

for all  $1 \leq i < p^m$ . Then we complete the proof by applying Lemma 16.  $\square$

*Proof of Lemma 10:* Fix a subset  $\Sigma$  of  $\mathbb{P}^N(K_v^{p^m})$  for some place  $v \in \Omega_K$  and some positive integer  $m$ , and denote by  $I_v$  the ideal in  $K_v[X_0, \dots, X_N]$  generated by homogeneous polynomials which vanish on  $\Sigma$ . Let  $f \in I_v$  be a homogeneous polynomial and  $P \in \Sigma$ . By the definition of  $D_{K_v}^{(i)}(f)$  and the assumption  $P \in \mathbb{P}^N(K_v^{p^m})$ , we have  $0 = D_{K_v}^{(i)}(f(P)) = D_{K_v}^{(i)}(f)(P)$  for each  $1 \leq i < p^m$ . This shows  $D_{K_v}^{(i)}(I_v) \subset I_v$  for all  $1 \leq i < p^m$ . Again, we complete the proof by using Lemma 16.

#### ACKNOWLEDGEMENTS

I thank the referee for his/her careful comments on an earlier version of this paper, which generalizes a part of my dissertation completed under the advising of José Felipe Voloch. Also, I appreciate that Andreas Schweizer, Ki-Seng Tan, and Julie Wang made many useful suggestions on my revision. Especially, I am grateful to Tan for showing me examples of succinct writing.

#### REFERENCES

- [AV92] Dan Abramovich and José Felipe Voloch. Toward a proof of the Mordell-Lang conjecture in characteristic  $p$ . *Internat. Math. Res. Notices*, (5):103–115, 1992.
- [Che51] Claude Chevalley. Deux théorèmes d'arithmétique. *J. Math. Soc. Japan*, 3:36–44, 1951.
- [GV87] Arnaldo García and J. F. Voloch. Wronskians and linear independence in fields of prime characteristic. *Manuscripta Math.*, 59(4):457–469, 1987.
- [HR79] Edwin Hewitt and Kenneth A. Ross. *Abstract harmonic analysis*, volume 1. Springer-Verlag, New York, 1979.

- [MB81] L. Moret-Bailly. Familles de courbes et de variétés abéliennes sur  $\mathbb{P}^1$ . *Séminaire sur les pinceaux de courbes de genre au moins deux*, *Astérisque*, 86, 1981.
- [Mil72] James Stuart Milne. Congruence subgroups of abelian varieties. *Bull. Sci. Math. (2)*, 96:333–338, 1972.
- [Mil06] J. S. Milne. *Arithmetic duality theorems*. BookSurge, LLC, Charleston, SC, second edition, 2006.
- [Ogu78] Arthur Ogus.  $F$ -crystals and Griffiths transversality. In *Proceedings of the International Symposium on Algebraic Geometry (Kyoto Univ., Kyoto, 1977)*, pages 15–44, Tokyo, 1978. Kinokuniya Book Store.
- [PV10] Bjorn Poonen and José Felipe Voloch. The Brauer-Manin obstruction for subvarieties of abelian varieties over function fields. *Ann. of Math. (2)*, 171(1):511–532, 2010.
- [Sch39] Friedrich Karl Schmidt. Die Wronskische Determinante in beliebigen differenzierbaren Funktionenkörpern. *Math. Z.*, 45(1):62–74, 1939.
- [Ser71] Jean-Pierre Serre. Sur les groupes de congruence des variétés abéliennes. II. *Izv. Akad. Nauk SSSR Ser. Mat.*, 35:731–737, 1971.
- [Ser88] Jean-Pierre Serre. *Algebraic groups and class fields*, volume 117 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1988. Translated from the French.
- [Tat95] John Tate. On the conjectures of Birch and Swinnerton-Dyer and a geometric analog. In *Séminaire Bourbaki, Vol. 9*, pages Exp. No. 306, 415–440. Soc. Math. France, Paris, 1995.